IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

CHRIS IZQUIERDO, individually and on behalf of all others similarly situated, Plaintiff, v. MATERNAL & FAMILY HEALTH SERVICES, INC. Defendant.	Case No. CIVIL ACTION – CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Chris Izquierdo, individually and on behalf of the Class defined below of similarly situated persons, brings this Class Action Complaint and alleges the following against Maternal & Family Health Services ("MFHS" or "Defendant"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. Plaintiff brings this class action against MFHS for MFHS's failure to properly secure and safeguard protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information, including without limitation names, dates

of birth, Social Security numbers, medical record and patient account numbers, health insurance information, diagnoses, medication information, treatment providers, types of treatment, and treatment locations (collectively, "PHI"), for failing to comply with industry standards to protect information systems that contain that PHI, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PHI had been compromised. Plaintiff seeks, among other things, orders requiring MFHS to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future.

2. MFHS is a leading healthcare provider in Pennsylvania for women, children and families.

3. On or about April 4, 2022, MFHS announced a security incident that occurred between August 2021 and April 2022, involving PHI (the "Data Breach"). The Data Breach was wide-reaching and compromised the PHI of at least 461,000 individuals, according to the submission MFHS made to the U.S. Secretary of Health and Human Services at the Office for Civil Rights ("OCR").[1]

[1] Department of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed January 16, 2023).

4. MFHS began notifying, via U.S. Mail, potentially affected individuals including certain current and former employees, patients and vendors on January 3, 2023.

5. This case involves a breach by an unknown third party, resulting in the unauthorized disclosure of the PHI of Plaintiff and Class Members by MFHS to unknown third parties. As a result of MFHS's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PHI is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to MFHS's failures.

6. Additionally, as a result of MFHS's failure to follow contractually agreed upon, federally prescribed, industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services MFHS was to provide. MFHS expressly represented that it would maintain the confidentiality of Plaintiff and Class Members' PHI obtained throughout the course of treatment.

7. Accordingly, Plaintiff, individually and on behalf of all others similarly situated, alleges claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, and breach of confidence.

PARTIES

8. Plaintiff is a citizen and resident of Scranton, Pennsylvania. Plaintiff was a patient of MFHS. Plaintiff's PHI was disclosed without authorization to an unknown third party as a result of the Data Breach.

9. Defendant MFHS is a leading private, not-for-profit Pennsylvania healthcare system with its principal address at 15 Public Square, Suite 600, Wilkes-Barre, PA, 18701.

10. MFHS cares for women, children and families through a network of facilities, primary and specialty care practices located in the Commonwealth of Pennsylvania. Due to the nature of these services, MFHS collects and electronically stores patient PHI.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C.§ 1332 (d). The amount in controversy exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred putative class members, and at least one putative class member is a citizen of a different state than Defendant.

12. MFHS regularly and systematically conducted and continues to conduct in in 17 counties throughout northeastern Pennsylvania.

13. This Court has personal jurisdiction over MFHS because MFHS maintains its principal place of business in this jurisdiction and is authorized to and does conduct substantial business in this jurisdiction.

14. Venue is proper in this Court because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, MFHS is based in this District, MFHS maintains patients' PHI in this District, and has caused harm to Plaintiff and Class Members residing in this District.

FACTUAL BACKGROUND

A. MFHS's Business

15. Defendant began operating as a healthcare facility in Pennsylvania in 1971.[2]

16. MFHS's facilities consist of several facilities including family planning centers, medical centers and community health centers, located in the northeastern Pennsylvania region. MFHS serves over 900,000 women, men, and children annually.[3]

[2] *See* https://www.mfhs.org/about-us/ (last accessed Jan.16, 2023).

[3] *See id.*

17. As a healthcare provider, MFHS is required to ensure that such private, personal information is not disclosed or disseminated to unauthorized third parties without the patients' express written consent, as further detailed below.

B. The Data Breach

18. On April 4, 2022, MFHS identified a ransomware incident that resulted in the exposure of sensitive information to an unauthorized individual.[4]

19. After engaging a computer forensic firm to investigate the suspicious activity, MFHS determined that an unauthorized third party gained access to the MFHS's systems between August 21, 2021 and April 4, 2022.

20. The investigation concluded that through this unauthorized access, the unauthorized third party had access to sensitive patient PHI including at least: names, dates of birth, medical record and patient account numbers, driver's license numbers, payment and financial account information, health insurance information, and other medical information.

21. MFHS concluded that patient Social Security numbers were also compromised.

[4] *See* https://www.mfhs.org/important-information-about-maternal-family-health-services-2022-cybersecurity-incident/ (last accessed Feb. 28, 2023).

22. On January 3, 2023, MFHS began mailing letters to affected individuals including certain current and former employees, patients and vendors whose information was identified as compromised.

23. The letters Plaintiff and Class Members received were untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, why sensitive patient information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether MFHS knows if the data has not been further disseminated.

24. In deliberate disregard of the fact that the stolen sensitive information was accessed by an unauthorized third party, MFHS downplayed the seriousness of the incident by telling Plaintiff and Class Members, without any way to support the veracity, that there is no evidence at this time that any personal information has been misused as a result of the incident. *See*, Exhibit A, Breach Notification Letter.

25. These representations are boilerplate language suggesting MFHS's lack of concern for the seriousness of the Data Breach—wherein an unauthorized third party gained access to PHI in MFHS's possession.

26. To date, MFHS has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, MFHS has

taken to secure the PHI still in its possession. Through this litigation, Plaintiff and Class Members seek to determine the scope of the Data Breach and the information involved, obtain relief that redresses Plaintiff's and Class Members' harms, and ensure MFHS has proper measures in place to prevent another breach from occurring in the future.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

27. MFHS was on notice that companies in the healthcare industry are susceptible targets for data breaches.

28. MFHS was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[5] The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

[5] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last accessed Jan. 16, 2023).

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.

29. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[6] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[7] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[8]

---

[6] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed Jan. 16, 2023).

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Jan. 16, 2023).

[8] *Id.*

30. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[9]

31. As the number of healthcare data breaches continues to rise, email remains the primary outlet through which health data is exposed. For example, in 2017, there were 85 reported email-related healthcare breaches—more than double the number reported in 2016—accounting for nearly one-quarter of all healthcare breaches.[10]

32. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that

[9] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed Jan. 16, 2023).

[10] Jessica Kim Cohen, *Email Is Now the Top Source of Healthcare Breaches*, Modern Healthcare (Mar. 23, 2019), *available at*: https://www.modernhealthcare.com/technology/email-now-top-source-healthcare-breaches (last accessed Jan. 16, 2023).

> cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[11]

33. In the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"[12]

34. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's on-going training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[13]

35. ProtonMail Technologies publishes a guide for IT Security to small businesses (i.e., companies without the heightened standard of care applicable in the healthcare industry). In its 2019 guide, ProtonMail dedicates a full chapter of its

---

[11] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Jan. 16, 2023).

[12] Aaron Jensen, Healthcare Phishing Statistics: 2019 HIMSS Survey Results (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results (last visited Jan. 16, 2023).

[13] *Id.*

Book guide to the danger of phishing and ways to prevent a small business from falling prey to it. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[14]

As a major healthcare provider, MFHS knew, or should have known, the importance of safeguarding the patients' PHI entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on MFHS's patients as a result of a breach. MFHS failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. MFHS Obtains, Collects, and Stores Plaintiff's and Class Members' PHI

36. MFHS obtains, collects, and stores a massive amount of its patients' protected health information and personally identifiable data.

[14] *The ProtonMail Guide to IT Security for Small Businesses*, ProtonMail (2019), *available at* https://protonmail.com/it-security-complete-guide-for-businesses (last visited Jan. 16, 2023).

37. As a condition of engaging in health services, MFHS requires that patients entrust it with highly confidential PHI.

38. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PHI, MFHS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' PHI from disclosure.

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PHI and, as current and former patients, they rely on MFHS to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

E. The Value of PHI and the Effects of Unauthorized Disclosure

40. MFHS was well aware that the information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

41. PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[15] Indeed, a robust cyber

[15] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Jan. 16, 2023).

black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

42. While credit card information and associated personally identifiable information can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[16]

43. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

44. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions

[16] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Jan. 16, 2023).

and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[17]

45. The ramifications of MFHS's failure to keep its patients' PHI secure are long lasting and severe. Once PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

46. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [18] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[19]

47. Here, not only was sensitive medical information compromised, but also financial information and Social Security numbers. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected

---

[17] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://khn.org/news/rise-of-indentity-theft/ (last accessed Jan. 16, 2023).

[18] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed Jan. 16, 2023).

[19] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accessed Jan. 16, 2023).

until debt collection calls commence months, or even years, later.[20] This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

48. Stolen Social Security numbers make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

49. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

[20] *Identity Theft and Your Social Security Number*, Social Security Administrative *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 16, 2023).

50. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

51. MFHS knew, or should have known, the importance of safeguarding its patients' PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on MFHS's patients as a result of a breach. MFHS failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

52. The ramifications of MFHS's failure to keep its patients' PHI secure are long lasting and severe.

F. The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Monetary Injuries

53. The Breach Notification Letter from MFHS, attached hereto as Exhibit A, advised Plaintiff that her name, address, date of birth, Social Security Number, driver's license number, health insurance information, medical information, and payment card information were compromised in the Data Breach.

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Jan. 16, 2023).

54. This exposure disturbs Plaintiff and Class Members as they no longer control their highly sensitive medical records, cannot stop others from viewing it, and cannot prevent criminals from misusing it.

55. What's more, the Data Breach exposed Plaintiff and Class Members to an increased lifelong risk for identity theft and fraud. Indeed, the Data Breach included information patients cannot change, like Social Security numbers and birth dates.

56. Since the Data Breach, Plaintiff has suffered identity theft, fraud, and harm.

57. At least 5 fraudulent credit card accounts have been opened in Plaintiff's name since the Data Breach. Opening these accounts would have required knowledge of Plaintiff's personally identifiable information, such as name, date of birth, and Social Security number, all of which were compromised in the Data Breach.

58. Plaintiff's credit score has decreased as these fraudulent accounts have outstanding balances.

59. Additionally, the outstanding balances are accruing interest charges that Plaintiff has been asked to pay.

60. Further, a utility service account has been opened using Plaintiff's personally identifiable information in Florida, where Plaintiff has never lived.

61. To work through this fraud and identity theft, Plaintiff has devoted at least 80 hours to remediating it and mitigating the potential for it to happen again.

62. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. The fear stems from the fact that her highly sensitive PHI and PII is in criminal hands, who have already shown they will misuse her information. These emotional harms go far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

63. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

64. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

65. Plaintiff suffers a present injury from the increased risk of fraud, identity theft, and misuse resulting from her PHI being placed in the hands of criminals. Plaintiff has a continuing interest in ensuring that his PII and PHI, which is the type that cannot be changed and upon information and belief remains in Defendant's possession, is protected and safeguarded from future breaches.

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is

incurring and will continue to incur such damages in addition to any fraudulent use of their PHI.

67. Despite all of the publicly available knowledge of the continued compromises of PHI, MFHS's approach to maintaining the privacy of MFHS's patients' protected health information was lackadaisical, cavalier, reckless, or in the very least, negligent.

68. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of MFHS's misfeasance.

69. Once PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[22]

70. MFHS's delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiffs were not timely notified of the Data Breach, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

[22] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Jan. 16, 2023).

71. As a result of MFHS's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. Actual identity theft;

b. Unauthorized use and misuse of their PHI;

c. The loss of the opportunity to control how their PHI is used;

d. The diminution in value of their PHI;

e. The compromise, publication, and/or theft of their PHI;

f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Costs associated with placing freezes on credit reports;

i. Delay in receipt of tax refund monies;

j. The diminished value of MFHS's goods and services they received;

k. Lost opportunity and benefits of electronically filing of income tax

returns;

l. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PHI being placed in the hands of criminals;

m. The continued risk to their PHI, which remains in the possession of MFHS and is subject to further breaches so long as MFHS fails to undertake appropriate measures to protect the PHI in its possession; and

n. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

G. MFHS's Conduct Violates HIPAA

72. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions requirethat the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

73. MFHS's Data Breach resulted from a combination of insufficiencies that indicate MFHS failed to comply with safeguards mandated by HIPAA

regulations and industry standards. First, it can be inferred from MFHS's Data Breach that MFHS either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff's and Class Members' PHI.

74. Plaintiff' and Class Members' Personal and Medical Information is "protected health information" as defined by 45 CFR § 160.103.

75. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

76. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

77. Plaintiff's and Class Members' Personal and Medical Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

78. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

79. Based upon the breach notification letter, MFHS reasonably believes Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

80. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

81. MFHS reasonably believes Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

82. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

83. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

84. MFHS reasonably believes Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

85. It is reasonable to infer that Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

86. It should be rebuttably presumed that unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

87. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

88. In addition, MFHS's Data Breach could have been prevented if MFHS implemented HIPAA mandated, industry standard policies and procedures for

securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

89. MFHS's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information MFHS creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR

164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

90. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required MFHS to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[23]

[23] Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at*: hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Jan. 16, 2023).

91. Because MFHS has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure MFHS's approach to information security is adequate and appropriate. MFHS still maintains the protected health information and other sensitive information of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' PHI remains at risk of subsequent Data Breaches.

H. MFHS Failed to Comply with FTC Guidelines

92. MFHS was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

93. The Federal Trade Commission ("FTC") has promulgated guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into

all business decision-making.[24]

94. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[25] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

95. The FTC further recommends that companies not maintain PHI longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

96. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ

[24] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Jan. 16, 2023).

[25] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Jan. 16, 2023).

[26] FTC, *Start With Security*, *supra* note 16.

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

97. MFHS failed to properly implement basic data security practices. MFHS's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

98. MFHS was at all times fully aware of its obligation to protect the PHI of patients because of its position as a leading healthcare provider. MFHS was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

99. Plaintiff brings this suit as a class action on behalf of herself and on behalf of all others similarly situated.

100. The Class that Plaintiff seeks to represent is defined as follows:

> **All individuals whose PHI was compromised in the MFHS Healthcare Network Data Breach which occurred from August 2021 to April 2022.**

101. Excluded from the Class are the officers, directors, and legal

representatives of MFHS, and the judges and court personnel in this case and any members of their immediate families.

102. Plaintiff reserves the right to modify or amend the definition of the proposed Class as additional information becomes available to plaintiff.

103. Numerosity. The Class Members are so numerous that joinder of all Members is impractical. The Class is comprised of at least 461,000 patients.

104. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PHI of Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff' and Class Members' PHI;

c. Whether Defendant had duties not to disclose the PHI of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff' and Class Members' PHI;

e. Whether Defendant failed to adequately safeguard the PHI of Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in

handling Plaintiff' and Class Members' PHI by storing that information on unsecured servers;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiff and Class Members on the other;

i. Whether Defendant had respective duties not to use the PHI of Class Members for non-business purposes;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI had been compromised;

k. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

o. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

p. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and

q. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

105. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI, like that of every other Class Member, was disclosed by MFHS. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of MFHS. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

106. Policies Generally Applicable to the Class. This class action is also appropriate for certification because MFHS has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. MFHS's policies challenged herein apply to and affect Class Members uniformly and Plaintiff' challenge of these policies hinges on MFHS's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

107. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no disabling conflicts

of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation and in particular privacy class litigation, and Plaintiff intends to prosecute this action vigorously.

108. Superiority of Class Action. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like MFHS. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

109. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged

because MFHS would necessarily gain an unconscionable advantage since MFHS would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

110. The litigation of the claims brought herein is manageable. MFHS's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

111. Adequate notice can be given to Class Members directly using information maintained in MFHS's records.

112. Unless a Class-wide injunction is issued, MFHS may continue in its failure to properly secure the PHI of Class Members, MFHS may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and MFHS may continue to act unlawfully as set forth in this Complaint.

113. Further, MFHS has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

114. Plaintiff realleges paragraphs 1 through 114 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

115. As a condition of their utilizing the services of MFHS, patients were obligated to provide MFHS with certain PHI, including their dates of birth, Social Security numbers, financial information, personal medical information, and other protected health information.

116. Plaintiff and the Class Members entrusted their PHI to MFHS on the premise and with the understanding that MFHS would safeguard their information, use their PHI for business purposes only, and/or not disclose their PHI to unauthorized third parties.

117. MFHS has full knowledge of the sensitivity of PHI and the types of harm that Plaintiff and Class Members could and would suffer if PHI was wrongfully disclosed.

118. MFHS knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of patients' PHI involved an

unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

119. MFHS had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing MFHS's security protocols to ensure that Plaintiff's and Class Members' information in MFHS's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on security measures regarding the security of patients' personal and medical information.

120. MFHS had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PHI.

121. Additionally, violations of statutes which establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence *per se.*

122. Section 5 of the FTC Act prohibits ""unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as MFHS, of failing to use reasonable measures to protect PHI. The FTC publications and orders described above also form part of the basis of MFHS's duty in this regard.

123. MFHS violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PHI and not complying with applicable industry standards, as described in detail herein. MFHS's conduct was particularly unreasonable given the nature and amount of PHI they obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

124. MFHS's violation of Section 5 of the FTC Act constitutes negligence *per se.*

125. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

126. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

127. MFHS's violations of HIPAA also independently constitute negligence *per se*.

128. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA

privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

129. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

130. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

131. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of the growing amount of data breaches for health care providers and other industries.

132. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. MFHS knew or should have known of the inherent risks in collecting and storing the PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PHI, and that it had inadequate employee training and education and IT security protocols in place to secure the PHI of Plaintiff and the Class.

133. MFHS's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. MFHS's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

MFHS's misconduct also included its decisions not to comply with industry standards for the safekeeping and unauthorized disclosure of the PHI of Plaintiff and Class Members.

134. Plaintiff and the Class Members had no ability to protect their PHI that was in MFHS's possession.

135. MFHS was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

136. MFHS had and continues to have a duty to adequately disclose that the PHI of Plaintiff and Class Members within MFHS's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI by third parties.

137. MFHS has admitted that the PHI of Plaintiff and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

138. MFHS, through its actions and/or omissions, unlawfully breached MFHS's duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PHI of Plaintiff and Class Members during the time the PHI was within MFHS's possession or control.

139. MFHS improperly and inadequately safeguarded the PHI of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

140. MFHS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PHI.

141. MFHS, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

142. But for MFHS's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PHI of Plaintiff and Class Members would not have been compromised.

143. There is a close causal connection between MFHS's failure to implement security measures to protect the PHI of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PHI was accessed as the proximate result of MFHS's failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

144. As a direct and proximate result of MFHS's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in MFHS's possession and is subject to further unauthorized disclosures so long as MFHS fails to undertake appropriate and adequate measures to protect the PHI of patients and former patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of MFHS's goods and services Plaintiff and Class Members received.

145. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SECOND CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff and the Class)

146. Plaintiff realleges paragraphs 1 through 114 above as if fully set forth herein.

147. As a healthcare provider, MFHS entered into contracts with Plaintiff and Class Members.

148. The promises and representations described above relating to HIPAA and other industry practices, and about MFHS's purported concern about its patients' privacy rights became terms of the contract between MFHS and its patients, including Plaintiff and Class Members.

149. MFHS breached these promises by failing to comply with HIPAA and other reasonable industry practices.

150. Plaintiff and Class Members fully performed their obligations under the contracts with MFHS. MFHS breached its agreements with Plaintiff and Class Members by failing to protect their PHI. Specifically, MFHS: (1) failed to take reasonable steps to use safe and secure systems to protect PHI; (2) failed to have appropriate security protocols and measures in place; (3) allowed unauthorized third parties to gain access to patients' PHI; and (4) failed to promptly alert or give notice of the Data Breach to Plaintiff and Class Members.

151. As a result of MFHS's breach of these terms, Plaintiff and Class

Members have been harmed and put at risk of future harm.

152. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

153. Plaintiff realleges paragraphs 1 through 116 above as if fully set forth herein.

154. Plaintiff and Class Members were required to provide their PHI, including names, Social Security numbers, dates of birth, medical histories, and other personal information to MFHS as a condition of their use of MFHS's services.

155. Plaintiff and Class Members paid money to MFHS in exchange for goods and services, as well as MFHS's promises and obligations to protect PHI from unauthorized disclosure.

156. By providing public healthcare services, Defendant expressly promised Plaintiff and Class Members that Defendant would only disclose protected health information and sensitive information under certain circumstances, none of which relate to the Data Breach.

157. By providing public healthcare services, Defendant promised to comply with HIPAA standards and to make sure that Plaintiff' and Class Members'

protected health information would remain protected.

158. Implicit in the agreement between MFHS's patients, including Plaintiff and Class Members, to provide PHI, and MFHS's acceptance of such PHI, was MFHS's obligation to use the PHI of its patients for business purposes only, take reasonable steps to secure and safeguard that PHI, and not make unauthorized disclosures of the PHI to unauthorized third parties.

159. Further, implicit in the agreement, MFHS was obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other PHI.

160. Without such implied contracts, Plaintiff and Class Members would not have provided their PHI to MFHS.

161. MFHS had an implied duty to reasonably safeguard and protect the PHI of Plaintiff and Class Members from unauthorized disclosure or uses.

162. Additionally, MFHS implicitly promised to retain this PHI only under conditions that kept such information secure and confidential.

163. Plaintiff and Class Members fully performed their obligations under the implied contract with MFHS; however, MFHS did not.

164. MFHS breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' PHI, which was compromised as a result of the Data Breach.

165. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise to abide by HIPAA.

166. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information MFHS created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

167. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

168. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

169. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

170. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards

to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

171. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

172. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

173. MFHS further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

174. MFHS further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

175. MFHS further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff' and Class Members' PHI.

176. MFHS's failures to meet these promises constitute breaches of the implied contracts.

177. Because MFHS allowed unauthorized access to Plaintiff's and Class Members' PHI and failed to safeguard the PHI, MFHS breached its contracts with Plaintiff and Class Members.

178. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete PHI and to pay MFHS in exchange for MFHS's agreement to, *inter alia*, protect their PHI.

179. MFHS breached its contracts by not meeting the minimum level of protection of Plaintiff's and Class Members' PHI.

180. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in MFHS providing goods and services to Plaintiff and Class Members that were of a diminished value.

181. As a direct and proximate result of MFHS's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort

expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in MFHS's possession and is subject to further unauthorized disclosures so long as MFHS fails to undertake appropriate and adequate measures to protect the PHI of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of MFHS's goods and services they received.

182. As a direct and proximate result of MFHS's breach of its implied contracts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

183. Plaintiff realleges paragraphs 1 through 114 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

184. In light of the special relationship between MFHS and its patients, whereby MFHS became a guardian of Plaintiff's and Class Members' highly sensitive, confidential, personal, financial information, and other PHI, MFHS was a fiduciary, created by its undertaking and guardianship of the PHI, to act primarily for the benefit of its patients, including Plaintiff and Class Members, for: (1) the safeguarding of Plaintiff's and Class Members' PHI; (2) timely notifying Plaintiff and Class Members of a data breach or disclosure; and (3) maintaining complete and accurate records of what and where MFHS's patients' information was and is stored.

185. MFHS had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its patients' relationship, in particular to keep secure the PHI of its patients.

186. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to diligently investigate the Data Breach to determine the number of Members affected in a reasonable and practicable period of time.

187. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to protect Plaintiff's and Class Members' PHI.

188. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

189. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information MFHS created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

190. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

191. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

192. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

193. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security

or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

194. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

195. MFHS breached its fiduciary duties to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94).

196. MFHS breached its fiduciary duties to Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

197. As a direct and proximate result of MFHS's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and

attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI, which remain in MFHS's possession and is subject to further unauthorized disclosures so long as MFHS fails to undertake appropriate and adequate measures to protect the PHI of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of MFHS's goods and services they received.

198. As a direct and proximate result of MFHS's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of Plaintiff and the Class)

199. Plaintiff realleges paragraphs 1 through 114 above as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

200. Plaintiff and Class Members have an interest, both equitable and legal,

in the PHI about them that was conveyed to, collected by, and maintained by MFHS and that was ultimately accessed or compromised in the Data Breach.

201. As a healthcare provider, MFHS has a fiduciary relationship to its patients, like Plaintiff and the Class members.

202. Because of that special relationship, MFHS was provided with and stored private and valuable PHI related to Plaintiff and the Class which it had a duty to maintain such information in confidence.

203. Patients like Plaintiff and Class members have a privacy interest in personal medical matters, and MFHS had a duty not to disclose medical data concerning its patients.

204. As a result of the parties' relationship, MFHS had possession and knowledge of confidential PHI and confidential medical records of Plaintiff and Class members, information not generally known.

205. Plaintiff and Class members did not consent to nor authorize MFHS to release or disclose their PHI to an unknown criminal actor.

206. MFHS breached its duty of confidences owed to Plaintiff and Class Members. MFHS breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PHI; (b) mishandling its data security

by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff' and Class members' PHI and medical information to a criminal third party.

207. But for MFHS's wrongful breach of its duty of confidences owed to Plaintiff and Class Members, their privacy, confidences, PHI would not have been compromised.

208. As a direct and proximate result of MFHS's breach of its duty, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the MFHS Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts by the Plaintiff, the Class and/or their parents or guardians;

f. The ongoing, imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PHI entrusted, directly or indirectly, to MFHS with the mutual understanding that MFHS would safeguard Plaintiff' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PHI, which remains in MFHS's possession and is subject to further breaches so long as MFHS fails to undertake appropriate and adequate measures to protect Plaintiff' and Class Members' data;

i. Loss of their privacy and confidentiality in their PHI;

j. The erosion of the essential and confidential relationship between MFHS – as a health care services provider – and Plaintiff and Class members as patients; and

k. Loss of personal time spent by the Plaintiff, the Class and/or their parents or guardians carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by MFHS.

209. Additionally, MFHS received payments from or on behalf of Plaintiff and Class members for services with the understanding that MFHS would hold in confidences Plaintiff' and Class members' private medical information.

210. MFHS breached the confidences of Plaintiff and Class members when it made an unauthorized release and disclosure of their confidential medical information and/or PHI.

211. It would be inequitable for MFHS to retain the benefit at Plaintiff' and Class members' expense.

212. As a direct and proximate result of MFHS's breach of its duty of confidences, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of herself and all others similarly situated, pray for relief as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PHI collection, storage, and protection, to disclose with specificity to Class Members the type of PHI compromised and enjoining Defendant's conduct requiring it to implement proper data security practices, specifically:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and laws;

iii. requiring Defendant to delete, destroy, and purge the PHI of Plaintiff and the Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff' and the Class members' PII/PHI;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating

firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI, as well as protecting the PHI of Plaintiff and the Class members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PHI;

xiii. requiring Defendant to implement, maintain, regularly review, and

revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PHI to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvi. requiring Defendant to design, maintain, and test its computer systems to ensure that PII/PHI in its possession is adequately secured and protected;

xvii. requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xix. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xx. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members.

d. For an award of damages, including actual, nominal, and consequential

damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Respectfully submitted,

Date: March 3, 2023

By: _____
Daniel L. Penetar III
GAZDA PENETAR, P.C.
753 East Drinker Street
Dunmore, Pennsylvania 18512
(570) 343-1141
dlp@gazdapenetar.com

BY: /s/ Francesca Kester Burne

MORGAN & MORGAN COMPLEX LITIGATION GROUP
Francesca Kester Burne
Jean S. Martin*
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
fkester@forthepeople.com
jeanmartin@forthepeople.com

Attorneys for Plaintiff and the Proposed Class

**Pro Hac Vice Application forthcoming*